(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 November 2006 (23.11.2006)

PCT

(10) International Publication Number
WO 2006/123899 A1

(51) International Patent Classification:
G06F 15/00 (2006.01)

(21) International Application Number:
PCT/KR2006/001852

(22) International Filing Date: 18 May 2006 (18.05.2006)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2005-0041431 18 May 2005 (18.05.2005) KR

(71) Applicant *(for all designated States except US)*: **SOL-MAZE CO., LTD.** [KR/KR]; No. 1212, Kolong Digital Tower, 222-7, Guro 3-dong, Guro-gu, Seoul 152-777 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **YANG, Ki-ho** [KR/KR]; 126-26, Daesin-dong, Seodaemun-gu, Seoul 120-160 (KR). **HWANG, Jay-Yeob** [KR/KR]; 106-dong, 703-ho, 1555, Bunji-joongsan village, Ilsan 2 -dong, Ilsan-gu, Goyang-si, Gyunggi-do 411-728 (KR).

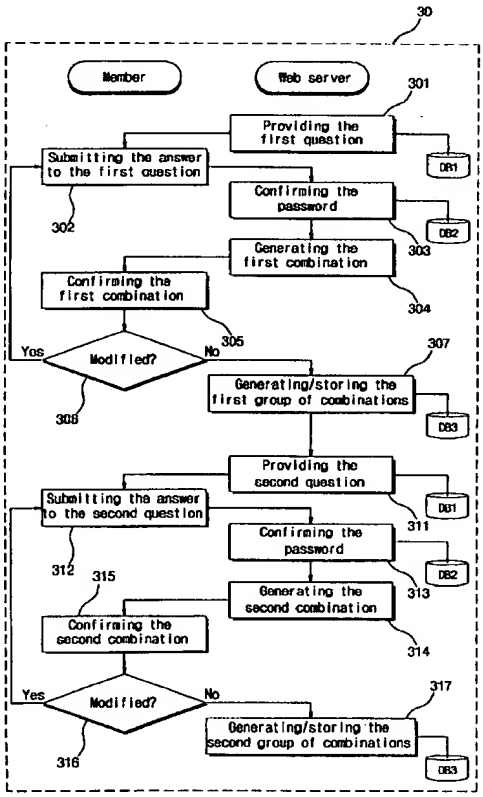
(74) Agent: **LEE, In sik**; No. 608, Geumsan Bldg., 17-1, Yeouido-dong, Yeongdeungpo-gu, Seoul 150-727 (KR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR OPERATING AND AUTHENTICATING PASSWORD SYSTEM, AND STORAGE MEDIA HAVING PROGRAM SOURCE THEREOF



(57) Abstract: Disclosed are a method for operating and authenticating a password system and storage media storing a program source thereof. This method includes a first step in which a user terminal requests a group of question-answer-hint combinations to a web server in order to confirm a password of a specific membership ID, and a second step in which, upon receipt of the request, the web server provides the user terminal with a first group of question-answer-hint combinations including a first question-answer-hint combination corresponding to a first character of the password and a second group of question-answer-hint combinations including a second question-answer-hint combination corresponding to a second character of the password. The method of the present invention has an advantage in that it provides an authenticating process on the website without collecting any personal information while having the same level of security compared to that of a password, hiding the meaning even from a website administrator, and assuring high reliability on the authentication of users on the website, and storage media storing a program source of the method.

WO 2006/123899 A1

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

【DESCRIPTION】

【Invention Title】

METHOD FOR OPERATING AND AUTHENTICATING PASSWORD SYSTEM, AND STORAGE MEDIA HAVING PROGRAM SOURCE THEREOF

【Technical Field】

The present invention relates to a method for operating and authenticating a password system and storage media storing a program source thereof, and more particularly, to a method for operating and authenticating a password system which provides an authenticating process on the website without collecting any personal information while having the same level of security compared to that of a password, hiding the meaning even from a website administrator, and assuring high reliability on the authentication of users on the website, and storage media storing a program source of the method.

【Background Art】

Nowadays, it is widespread that numerous websites managed by a membership system require visitors to join the website by inputting their own IDs and passwords.

There are plenty of websites using the membership system. Therefore, when a long time has been passed since a member had set up an initial password and had not visited the website afterward, there is frequently arisen an event of forgetting a password inputted at the moment of joining the website.

In this case, the existing solutions for authenticating the member and reissuing a password are as follows.

First of all, there is a method of asking the member's background information derived by his/her own experience.

FIG. 1 shows an example of a process of inputting background information on the membership website and FIG. 2 illustrates a process of confirming the background information inputted through the process presented in FIG. 1.

As shown in FIG. 1, according to the current membership website, in order to join the website a member is required to select any one of questions, for example, 'what is your most memorable place?', 'what is your favorite motto?', 'what is your most valuable thing?', 'what's the name of your most memorable teacher?' and so on, and write an

answer to the selected question based on his/her own experience.

Then, the website stores the background information written by the member in a membership management database, and then, validates the member by means of the method given in FIG. 2 when it needs to authenticate the member to issue a new password due to loss of a previously registered password. According to the example described in FIG. 2, it expects that the member inputs the background information on his/her birth place, already inputted when joining the membership website, for getting authentication.

By utilizing the personal information directly inputted by the member as information for authenticating the member, the membership website decreases the possibility that other person having none or small information on the member's private life does any act such as taking the password reissue by deceiving an administrator of the website as the member.

As another example of the authenticating process adopted by the membership websites, there exists a method of authenticating members via e-mail.

FIG. 3 illustrates a process of authenticating members by e-mail.

As exemplified in FIG. 3, although other person successfully answers to the question based on the member's personal experience, many membership websites send the password or temporary password via e-mail registered by the member, rather than offering the password immediately to the other person at that stage. In case of sending the temporary password, the member is required to go through the steps of logging with the temporary password and then changing it to a desired password.

The method of authentication based on the member's background information as explained in FIG. 1 and the method via e-mail as described in FIG. 3 have been used separately, but those two methods tend to be adopted for two-step confirmation in recent years.

In the case of passing through the two steps of authentication as such, since it appears that other person is not able to check out e-mail being sent to a designated address, it could be seen that the current password operating system, adopted by many membership websites, acquires some extent of security.

【Disclosure】

【Technical Problem】

However, the process of authentication in the current websites discussed above brings several problems as following.

Fundamentally, there are more problems except surreptitious use of the password and liability of failing authentication.

Firstly, the process of authentication for reissuing the password has a lower security level compared to the password itself.

The membership website operates the password system in order to validate a user with ID and the password thereof, and reissues the password through a given authenticating process in the case of forgetting the password. Thus, the security level of the authenticating process for reissuing the password should be at least equal to that of the password itself.

However, the current authenticating process described above allows others to get the password reissue by answering to the questions without the password or by sending a copy of other's identification card (in case of a real name system), thereby rendering other's ID used by stealth.

Secondly, a drawback is that personal information is drained and its surreptitious use is allowable.

In general, in case of failure in authentication on the membership website, there is no special way to log-in the website by using a present ID. Consequently, the problem of losing the member's own precious ID permanently happens due to the failure of authentication, so the real name membership system is preferred because it adopts an easier way to authenticate.

By the way, during the process of joining the real name membership on the website, it is general to collect personal information more than necessarily; and there is often occurred a problem of draining the collected personal information to unwanted places. Furthermore, there exists a problem that makes the drained personal information misused as information to use other's ID by stealth in the other websites again.

Thirdly, another problem is that there is no way of confirming whether to assure security of the authenticating process.

Likewise the security management of encoded password itself, information in the established process of authentication for the loss of the password should also have the

same level of security; and accordingly, the administrator of the website should not of course be allowed to be aware of the meaning of information in the process of authentication, even at its sight.

In general, however, issuing a new password by sending a copy of the member's identification card in case of loss of the password involves a problem, which is difficult to be solved by the existing authentication method, in which there exists a possibility for the administrator to store the personal information without decoding it and also for the administrator acquiring such information to use it by stealth anytime.

Due to these problems, there have been needs for the method of authenticating a password system which provides an authenticating process on the website without collecting any personal information while having the same level of security compared to that of a password, hiding the meaning even from a website administrator, and assuring high reliability on the authentication of users on the website, and storage media having a program source of the method.

【Technical Solution】

The present invention has been developed in order to solve the above problems, and it is, therefore, an object of the present invention to provide a method for operating and authenticating a password system which provides an authenticating process on the website without collecting any personal information while having the same level of security compared to that of a password, hiding the meaning even from a website administrator, and assuring high reliability on the authentication of users on the website, and storage media storing a program source of the method.

According to one aspect of the present invention to achieve the above object, there is provided a method of operating a password system, comprising: a first step of providing a user requesting authentication with a group of question-answer combinations including a question-answer combination corresponding to a specific membership ID; a second step of allowing the user to select one question-answer combination from the group of question-answer combinations in a multiple-choice manner; and a third step of authenticating the user as an owner of the specific membership ID if the selected question-answer combination is identical to the question-answer combination corresponding to the specific membership ID.

According to another aspect of the present invention, there is provided a method of operating a password system, comprising: a first step in which a user terminal requests a group of question-answer-hint combinations to a web server in order to confirm a password of a specific membership ID; and a second step in which, upon receipt of the request, the web server provides the user terminal with a first group of question-answer-hint combinations including a first question-answer-hint combination corresponding to a first character of the password and a second group of question-answer-hint combinations including a second question-answer-hint combination corresponding to a second character of the password.

In addition, it is preferable that each of the question-answer-hint combinations included in the group of question-answer-hint combinations has a different key cap image as a hint.

Also, it is preferable that a question of each of the question-answer-hint combinations is a graphic image and an answer thereto is a single comment inputted by an owner of the specific membership ID corresponding to the graphic image.

Or, it can be implemented in such a way that a question of each of the question-answer-hint combinations is a graphic image and an answer thereto does not exist separately.

Or, it can be implemented in such a way that a question of each of the question-answer-hint combinations is made in the form of text and an answer thereto is a simple sentence comment inputted by an owner of the specific membership ID corresponding to the question.

Meanwhile, the question-answer-hint combinations and the first and the second groups of question-answer-hint combinations are generated in advance before the first step and then stored in a membership information database.

More specifically, the first and the second question-answer-hint combinations and the first and the second groups of question-answer-hint combinations are generated and stored, before the first step, through the steps of: extracting first and second questions arbitrarily from a plurality of questions stored in a question database of the web server and providing the first and second questions to the user logged in a website with the specific membership ID; transmitting first and second answers written by the user in response to

the first and the second questions to the web server; generating the first question-answer-hint combination corresponding to the first question, the first answer and the first character of the membership ID and then the first group of question-answer-hint combinations having the first question-answer-hint combination and a plurality of question-answer-hint combinations except the first question-answer-hint combination, and the second question-answer-hint combination corresponding to the second question, the second answer and the second character of the membership ID and then the second group of question-answer-hint combinations having the second question-answer-hint combination and a multiplicity of question-answer-hint combinations except the second question-answer-hint combination; and storing the first and the second question-answer-hint combinations and the first and the second groups of question-answer-hint combinations in the membership information database.

In the above process, when the password is changed, the first question-answer-hint combination is changed to a new first question-answer-hint combination including a hint about a new first character of the password after change corresponding to the location of the first character of the password before change; a third question-answer-hint combination including the hint about the new first character among the first group of question-answer-hint combinations is changed to a new third question-answer-hint combination in which the hint about the new first character is replaced by the hint about the first character; the second question-answer-hint combination is changed to a new second question-answer-hint combination including a hint about a new second character of the password after change corresponding to the location of the second character of the password before change; and a fourth question-answer-hint combination including the hint about the new second character among the second group of question-answer-hint combinations is changed to a new fourth question-answer-hint combination in which the hint about the new second character is replaced by a keycap about the second character, all the changed combinations being stored in the membership information database.

According to still another aspect of the present invention, there is provided a computer-readable storage media having a password operating program source that is encoded and stored for computer access, comprising: a first process of providing a user requesting authentication with a group of question-answer combinations including a

question-answer combination corresponding to a specific membership ID; a second process of allowing the user to select one question-answer combination from the group of question-answer combinations in a multiple-choice manner; and a third process of authenticating the user as an owner of the specific membership ID if the selected question-answer combination is identical to the question-answer combination corresponding to the specific membership ID.

According to a further another aspect of the present invention, there is provided a computer-readable storage media having a password operating program source that is encoded and stored for computer access, comprising: a first process in which a user terminal of a membership website requests a group of question-answer-hint combinations to a web server in order to confirm a password of a specific membership ID; and a second process in which, upon receipt of the request, the web server provides the user terminal with a first group of question-answer-hint combinations including a first question-answer-hint combination corresponding to a first character of the password and a second group of question-answer-hint combinations including a second question-answer-hint combination corresponding to a second character of the password.

【Description of Drawings】

The above objects, features and advantages of the present invention will become more apparent from the following detailed description when taken in conjunction with the accompanying drawings, in which:

FIG. 1 illustrates an example of a process of inputting background information on a membership website;

FIG. 2 shows an example of a process confirming the background information inputted through the process described in FIG. 1;

FIG. 3 describes an example of a process of authenticating via e-mail;

FIG. 4 provides a flowchart of finding a lost password of a website member by using a method for operating a password system according to the present invention;

FIG. 5 is a flowchart illustrating details of the step of setting-up a password hint;

FIG. 6 shows a detailed flowchart of the step of providing the password hint;

FIG. 7 depicts an example of a first question-answer-hint combination according to the present invention;

FIG. 8 offers an example of a second question-answer-hint combination according to the present invention;

FIG. 9 shows an example of a first group of question-answer-hint combinations;

FIG. 10 depicts a first question-answer-hint combination;

FIG. 11 presents an example of a wrong question-answer-hint combination;

FIG. 12 describes an example of a second group of question-answer-hint combinations;

FIG. 13 shows an example of a second question-answer-hint combination;

FIG. 14 represents a process of inferring a complete password by using a keycap obtained from the first and the second question-answer-hint combinations; and

FIGs. 15 and 16 explain the concept of a maze-key scheme.

【Mode for Invention】

Although the present invention will now be described through preferred embodiments of a method of operating and authenticating a password system with reference to the accompanying drawings, the present invention is not limited to those embodiments.

[Embodiment 1]

Among methods of operating a password according to the present invention, an embodiment of a method of operating a password system implemented by using questions composed of graphic images will be described hereinafter.

FIG. 4 is a flowchart schematically showing a process of finding a lost password of a website member by using the password operating method according to an embodiment of the present invention.

As shown in FIG. 4, the process of finding the password based on the method 3 of the present invention comprises the three steps of: setting-up a password hint (30), providing a password hint (31), and reminding a password (32).

[Step of setting-up the password hint]

First of all, each member on the membership website makes a preparation for getting a password hint in advance against an event of forgetting the password in the step of setting-up password hint (30).

Thereafter, in the step of providing the password hint (31), members who forget

passwords for their own IDs in that website get parts of their own passwords based on the password hints established in the step of setting-up the password hint (30). For instance, there are provided as hints key cap images corresponding to certain characters arbitrarily assigned by the website or specific characters selected by members themselves among the characters constituting the passwords. The number of characters giving hints among the characters forming the passwords is not limited but can be one, or more than three. In the embodiment of the present invention, an example of getting the password hints for two characters will be described.

Since most people generally use limited numbers of passwords on the diverse websites, those members in the step of reminding the password (32) can easily remember their own passwords as a whole from the password hints provided by the step of providing the password hint (31).

FIG. 5 is a flowchart illustrating details of the step of setting-up the password hint (30).

As depicted in FIG. 5, a member sets up a password hint at the moment of joining the membership website, wherein at the first stage, the member gets a first question from the web server of the website (301). The first question is extracted arbitrarily from a question database DB1. According to the embodiment of the present invention, it is addressed that a picture (graphic image) is provided from the website and then comments thereon are written; and thus, the first question has the form of graphic image.

Thereafter, the member submits an answer to the first question, that is, his/her own comments on the graphic image after getting it from the website in the present embodiment (302). The comments come under the first answer corresponding to the first question.

In another embodiment of the present invention, it is possible to proceed to a next step 303, without performing the above step (302), that is, without commenting on the graphic image after getting it from the website. Due to the result of study on cognitive psychology that it takes a long time to completely forget a picture mindfully observed, it is allowable to implement another embodiment that doesn't need the above step (302).

After sending the first answer, the web server checks out the password of the member in reference to the membership information database DB2 (303). The reason why it checks the password is to create a first question-answer-hint combination for the

first question. That is, in the password checking step (303), the first character, which doesn't need to be the first character of the password as described above, is extracted from the password of the member.

The first question, the first answer and the extracted first character of the password, obtained from this process, are used to create the first question-answer-hint combination as a single body (304). In the embodiment of the present invention, the key cap image of a keyboard corresponding to the first character of the password is created to be linked as the hint.

Of course, in another embodiment excluding the above step (302), there exists no separate answer to the first question-answer-hint combination.

By sending the created first combination to the member in order to confirm it (305), it could be possible to give the member a chance to change the first answer if it is written with unwanted contents (306).

FIG. 7 offers an example of the first question-answer-hint combination according to the present invention. Referring to FIG. 7, only the question-answer combination is shown without the key cap image, i.e., the hint, according to the needs for security, in the confirming step (305).

In case where no more modification to the first question-answer-hint combination is needed, the web server generates a first group of question-answer-hint combinations by adding another question-answer-hint combination to the first question-answer-hint combination and stores the same in the membership information database DB2 (307).

Another question-answer-hint combination is selected randomly from other members' question-answer-hint combinations already stored in the membership information database DB2. At this time, the added question-answer-hint combination should include the image corresponding to the keycap, rather than the keycap corresponding to the member's first question-answer-hint combination. In general, since the number of keycaps representing characters is about 48, a total 48 question-answer-hint combinations including the first question-answer-hint combination can constitute the first group of question-answer-hint combinations in this embodiment.

Naturally, the member checked only the first question-answer-hint combination (305), and other 47 first question-answer-hint combinations remain to be unseen.

In this way, once the process of setting-up the first question-answer-hint combination and the first group of question-answer-hint combinations is completed, the process of setting-up a second question-answer-hint combination and a second group of question-answer-hint combinations is performed in the same manner, wherein details thereof are omitted here.

FIG. 8 shows an example of the second question-answer-hint combination according to the present invention. Like in FIG. 7, only the question-answer combination is presented, rather than hint (keycap image), in the checking step (315).

Through the above process, the member completes setting-up the password hint.

According to the present invention, a merit of the password hint established by the password operating method is that inputting the comments (the first answer) about the member's feeling for the picture (the first question) makes it easier to remember the password even after a long term on account of the member's sure recognition of the picture. Moreover, since the password hint is presented in a multiple-choice manner as mentioned later, the merit is maximized from the standpoints that doesn't need to remember details (e.g., spacing words) of the comments written in the step of setting-up the password hint.

Meanwhile, the member can modify the password after the step of setting-up the password hint, wherein there may be a question as to whether the password hint needs to be reestablished whenever modifying the password. The password operating method of the present invention, however, adopts a technique which changes the question-answer-hint combination into the characters corresponding to each position (the 1^{st}, the 2^{nd},..) of unmodified and modified passwords if any, and reorganizes the group of combinations in order to make other question-answer-hint combinations within that group of combinations have different keycaps from keycaps included in the question-answer-hint combination after modification.

Therefore, the password operating method of the present invention allows the status of setting-up the password hint to be maintained regardless of changing the password; and thus, the member can change the password as much as he/she wants.

[Step of providing the password hint]

Then, in the event of forgetting the password after setting-up the password hint, a process of providing the password hint will be described according to an example of the

password operating method of the present invention.

FIG. 6 is a flowchart presenting a detailed description of the step of providing the password hint (31).

As shown in FIG. 6, the step of providing password hint begins when the member who forgot the password requests provision of the password hint through an appropriate menu on the membership website (321). On this occasion, the member selects a password hint to be provided by inputting his/her membership ID.

The web server receiving a request for providing the password hint from the member searches the first group of question-answer-hint combinations corresponding to the membership ID in reference to the member information database DB2, and then provides the same to the member (322).

FIG. 9 shows an example of the first group of question-answer-hint combinations.

As shown in FIG. 9, 48 question-answer-hint combinations as many as the number of keycaps are provided on the screen of member's PC, wherein among them there exists only one question-answer-hint combination including the first answer directly written by the member.

If the member selects his/her own first question-answer-hint among the first group of question-answer-hint combinations, as shown in FIG. 10, it is possible to identify that the first keycap image of the password is a specific character included in the password. The thing different from FIG. 7 or 8 is that the hint (keycap image) can also be identified, in addition to the question-answer.

Likewise, the member identifies a second hint of the password by distinguishing the second question-answer-hint combination presented in FIG. 13 which is a second password hint, from the second group of question-answer-hint combinations represented on the screen of PC shown in FIG. 12.

As shown in FIG. 11, in case of selecting a wrong question-answer-hint combination, it is evident that due to receipt of a wrong hint the member cannot get any help to find the password.

Meanwhile, a description will be given on the reason why the question-answer-hint combination that provides a keycap image corresponding to the specific character not the specific character itself as a hint is used in the embodiment of the present invention,.

That is, there are too many expressible characters, which can be used as the password on the keyboard, such as English alphabet (capital and small letter), Korean characters, numerals, special characters (symbols), and further unique characters according to other languages. Consequently, in order to provide an adequate number of choices on the screen, it would be more proper to adopt the keycap image having about 48 numbers of occasions. Furthermore, the keycap image is sufficient to help users remember the password because they can generally remember which character is used as the password by presentation of the keycap image merely.

At this time, the number of question-answer-hint combinations constituting a group of question-answer-hint combinations needs to be exactly the same as, neither more nor less than, the number of keycap images representing the characters.

That is, while only one combination within the group of question-answer-hint combinations is familiar to the member who wants to get his/her own password hint and the other combinations are not all familiar to him/her, any combination among the group of question-answer-hint combinations is not familiar to others. Therefore, the viewpoint that the others can get no hint about the characters constituting the password is not entirely unlike pressing the arbitrary keyboard. As a result, the security of the password operating method according to the present invention remains intact. By the way, if the number of question-answer-hint combinations among the group of question-answer-hint combinations is more than that of the keycap images, there exist overlapping keycaps. Conversely, if the number of question-answer-hint combinations is less than that of the keycap images, there are missing keycaps. Therefore, the probability of selecting each keycap within that group of combinations is changed, thereby having a negative effect on the security of the password operating method of the present invention.

[Step of reminding the password]

By acquiring the keycaps corresponding to the first two characters of the forgotten password as hints through the process explained above, the member can infer the complete password, which himself/herself knows (32).

FIG. 14 represents the password inferring process, in which the member is able to easily infer the rest of the password frequently used after taking the keycap images corresponding to the first and the second password hints, respectively.

[Embodiment 2]

There was discussed in the first embodiment as described above the case where the question and the answer are made by the graphic image and the member's own comments on the graphic image, respectively.

Meanwhile, the password operating method according to the present invention is not limited to the case of setting-up the question and the answer to just the graphic image and the comments thereon, respectively.

The following second embodiment, therefore, deals with the case of setting-up each of the question and the answer in the form of text.

FIGs. 4 to 6 as shown above are used as references for the second embodiment as it is. But, it only needs to note that the question is replaced by the question having the form of text instead of the graphic image, and the answer is replaced by the answer to that question instead of the comments on the graphic image.

According to this embodiment, it can be seen that the question which is substantially the same as that in FIG. 1 can be utilized. However, even though the same question is utilized, the result is quite different from the case described in FIG. 1.

In other words, differently from the current authenticating process, although a long time has been passed since the member had set up the initial password, the possibility of failure to acquire password hints or authenticate due to trivial representative difference (e.g., spacing words) from the answer written before is considerably reduced because the member can get the password hint by simply selecting his/her own-written choice from multiple choices (the question-answer-hint combinations) through the step of providing the password hint.

In another modification of this embodiment, it can be possible that the system presents alliteration of two- or three-line poem instead of the question of text and the member inputs a line poem for the alliteration instead of inputting the answer to the question.

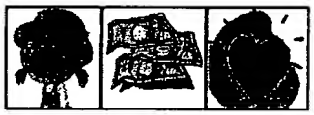
[Embodiment 3]

The applicant of the present invention has another patent application of Korean Patent Application No. 2004-81564, filed with Korean Intellectual Property Office on October 13, 2004, entitled "Safe Authentication Method," which is directed to a password

operating method using a maze-key scheme.

FIGs. 15 and 16 describe the concept of the maze-key scheme.

Hereinafter, the concept of the maze-key scheme will be simply explained with reference to FIGs. 15 and 16.

First of all, it is assumed that a specific member designates a maze-key of figures of  (woman-money-heart) and makes a memorizing formula "woman loves money" in order to memorize the maze-key.

In the password operating method using the maze-key scheme, a password is inputted by pressing direction keys of a keyboard in a logging process. Namely, as shown in FIG. 15, the direction keys are pressed to reach the second key of 'money' starting from the first key of 'woman', and likewise, to reach the last key of 'heart' starting from the key of 'money', wherein the first to the third keys are pre-designated by the member.

Meanwhile, since the member can forget these designated maze-keys in this password operating method using the maze-key scheme, it is necessary to provide hints of the maze keys against the case of forgetting them later.

In this case, the password operating method of the present invention can also be applied, like the other embodiments as mentioned above.

Each element (each key) constituting the maze-key can be the image as shown in FIG. 15 or 16, or numeral or character. Therefore, with regard to the image of each element key (or number/character) constituting the maze-key, it is possible to remember each element key forming the maze key in the same way as the first embodiment, by replacing the hint in the first embodiment as mentioned above by the image of each element key instead of the keycap image to generate a question-answer-hint combination and a group of question-answer-hint combinations including it.

Consequently, the password operating method according to the present invention can also be adopted in such a method using the maze-key scheme in order to provide the hint for remembering the maze-key in the case of forgetting the member's own maze-key.

[Other Embodiments]

If the picture provided in the first embodiment of the present invention is a 3D

rendering graphic image, the pictures (question) for obtaining the first and the second password hints offered in the step of providing the password hint can be replaced by the pictures observed in another angle or from different distance.

Moreover, it is also possible to apply the combination of the above various embodiments to the process of establishing the first and the second password hints. That is, the question-answer for the first password hint is made by combining the comments on the graphic image, and the question-answer for the second password hint is made by combining the answers to the question.

In the meantime, it is desirable to provide more hints, if necessary, by increasing the number of times of establishing and providing hints. Conversely, it is also desirable to provide a hint including a keycap image of many characters with only one request for the password hint by corresponding keycaps for more than two password characters to one question-answer combination.

As mentioned above, although the password operating method of the present invention has been described with reference to the specific embodiments, it is not to be restricted by the embodiments and figures. Namely, it is to be appreciated that those skilled in the art can change or modify the embodiments without departing from the scope and sprit of the present invention.

For example, the specific embodiments of the present invention as described above dealt with the case of website merely, but the password operating method of the present invention can also be applied to the password used in windows, mobile phones and so on.

【Industrial Applicability】

As described above, the present invention can implement a method for operating and authenticating a password system which provide an authenticating process on the website without collecting any personal information while having the same level of security compared to that of a password, hiding the meaning even from a website administrator, and assuring high reliability on the authentication of users on the website, and storage media storing a program source of the method.

【CLAIMS】

【Claim 1】 A method of operating a password system on a membership website, comprising:

a first step of providing a user requesting authentication with a group of question-answer combinations including a question-answer combination corresponding to a specific membership identification (ID);

a second step of allowing the user to select one question-answer combination from the group of question-answer combinations in a multiple-choice manner; and

a third step of authenticating the user as an owner of the specific membership ID if the selected question-answer combination is identical to the question-answer combination corresponding to the specific membership ID.

【Claim 2】 A method of operating a password system, comprising:

a first step in which a user terminal requests a group of question-answer-hint combinations to a web server in order to confirm a password of a specific membership ID; and

a second step in which, upon receipt of the request, the web server provides the user terminal with a first group of question-answer-hint combinations including a first question-answer-hint combination corresponding to a first character of the password and a second group of question-answer-hint combinations including a second question-answer-hint combination corresponding to a second character of the password.

【Claim 3】 The method according to claim 2, wherein each of the question-answer-hint combinations included in the first and the second groups of question-answer-hint combinations has a different key cap image as a hint.

【Claim 4】 The method according to claim 2, wherein a question of each of the question-answer-hint combinations is a graphic image and an answer to the question is a simple sentence comment inputted by an owner of the specific membership ID corresponding to the graphic image.

【Claim 5】 The method according to claim 2, wherein a question of each of the question-answer-hint combinations is a graphic image and an answer to the question does not exist separately.

【Claim 6】 The method according to claim 2, wherein a question of each of the

question-answer-hint combinations is made in the form of text and an answer to the question is a simple sentence comment inputted by an owner of the specific membership ID corresponding to the question.

【Claim 7】 The method according to any one of claims 4 to 6, wherein the first and the second question-answer-hint combinations and the first and the second groups of question-answer-hint combinations are generated in advance before the first step and then stored in a membership information database.

【Claim 8】 The method according to claim 7, wherein the first and the second question-answer-hint combinations and the first and the second groups of question-answer-hint combinations are generated and stored, before the first step, through the steps of:

extracting first and second questions arbitrarily from a plurality of questions stored in a question database of the web server and providing the first and second questions to the user logged in a website with the specific membership ID;

transmitting first and second answers written by the user in response to the first and the second questions to the web server;

generating the first question-answer-hint combination corresponding to the first question, the first answer and the first character of the membership ID and then the first group of question-answer-hint combinations having the first question-answer-hint combination and a plurality of question-answer-hint combinations except the first question-answer-hint combination, and the second question-answer-hint combination corresponding to the second question, the second answer and the second character of the membership ID and then the second group of question-answer-hint combinations having the second question-answer-hint combination and a multiplicity of question-answer-hint combinations except the second question-answer-hint combination; and

storing the first and the second question-answer-hint combinations and the first and the second groups of question-answer-hint combinations in the membership information database.

【Claim 9】 The method according to claim 8, wherein when the password is changed,

the first question-answer-hint combination is changed to a new first question-answer-hint combination including a hint about a new first character of the password after

change corresponding to the location of the first character of the password before change,

a third question-answer-hint combination including the hint about the new first character among the first group of question-answer-hint combinations is changed to a new third question-answer-hint combination in which the hint about the new first character is replaced by the hint about the first character,

the second question-answer-hint combination is changed to a new second question-answer-hint combination including a hint about a new second character of the password after change corresponding to the location of the second character of the password before change, and

a fourth question-answer-hint combination including the hint about the new second character among the second group of question-answer-hint combinations is changed to a new fourth question-answer-hint combination in which the hint about the new second character is replaced by a keycap about the second character, all the changed combinations being stored in the membership information database.

【Claim 10】 A computer-readable storage media having a password operating program source that is encoded and stored for computer access, comprising:

a first process of providing a user requesting authentication with a group of question-answer combinations including a question-answer combination corresponding to a specific membership ID;

a second process of allowing the user to select one question-answer combination from the group of question-answer combinations in a multiple-choice manner; and

a third process of authenticating the user as an owner of the specific membership ID if the selected question-answer combination is identical to the question-answer combination corresponding to the specific membership ID.

【Claim 11】 A computer-readable storage media having a password operating program source that is encoded and stored for computer access, comprising:

a first process in which a user terminal of a membership website requests a group of question-answer-hint combinations to a web server in order to confirm a password of a specific membership ID; and

a second process in which, upon receipt of the request, the web server provides the user terminal with a first group of question-answer-hint combinations including a first

question-answer-hint combination corresponding to a first character of the password and a second group of question-answer-hint combinations including a second question-answer-hint combination corresponding to a second character of the password.

Fig. 1

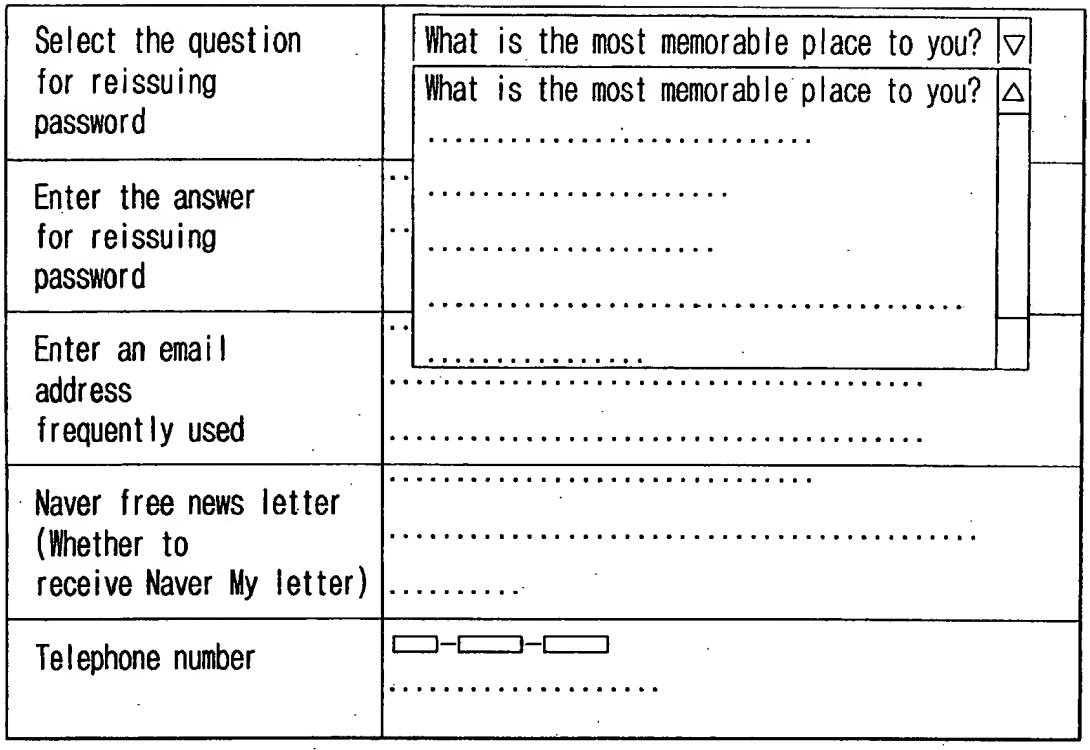

Select the question for reissuing password
What is the most memorable place to you?
What is the most memorable place to you?
Enter the answer for reissuing password
Enter an email address frequently used
Naver free news letter (Whether to receive Naver My letter)
Telephone number

Fig. 2

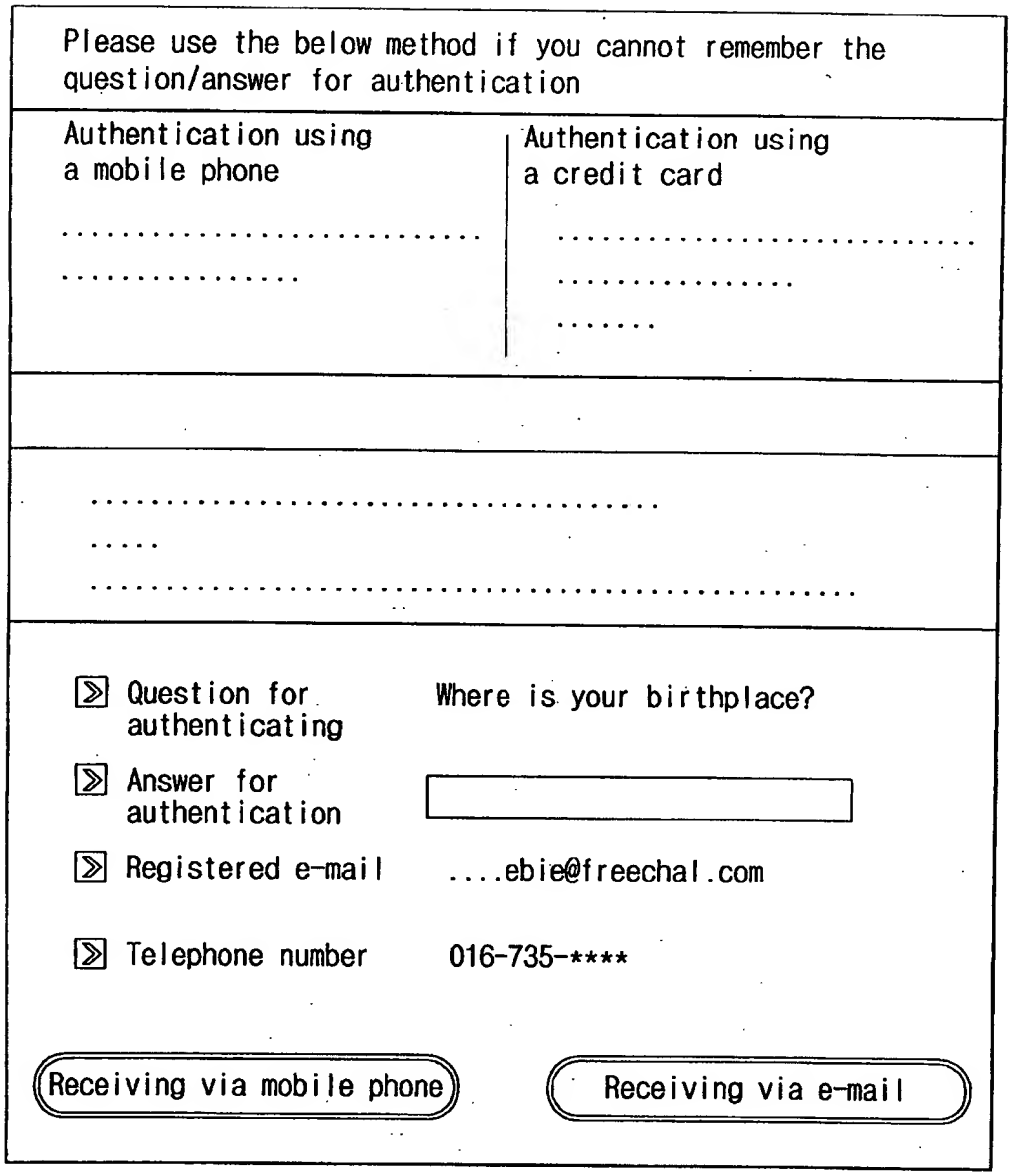

Please use the below method if you cannot remember the question/answer for authentication
Authentication using a mobile phone
Authentication using a credit card
Question for authenticating
Where is your birthplace?
Answer for authentication
Registered e-mail
....ebie@freechal.com
Telephone number
016-735-****
Receiving via mobile phone
Receiving via e-mail

Fig. 3

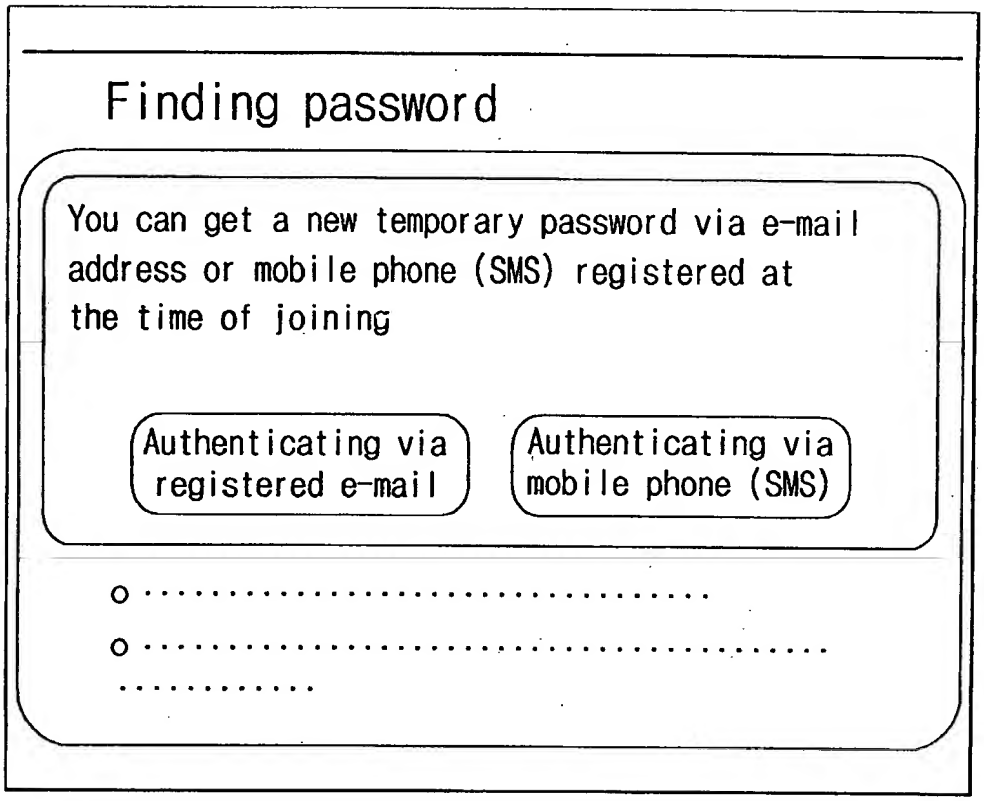

Finding password
You can get a new temporary password via e-mail address or mobile phone (SMS) registered at the time of joining
Authenticating via registered e-mail
Authenticating via mobile phone (SMS)
o .....
o .....
.....

Fig. 4

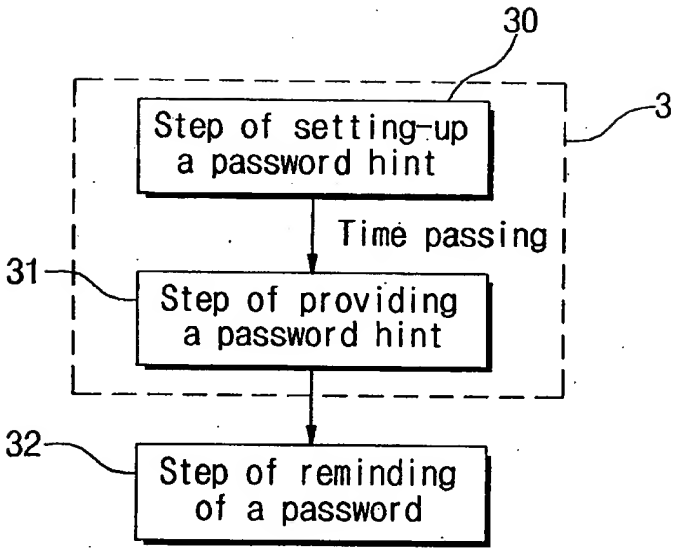

30
3
Step of setting-up a password hint
Time passing
31
Step of providing a password hint
32
Step of reminding of a password

Fig. 5

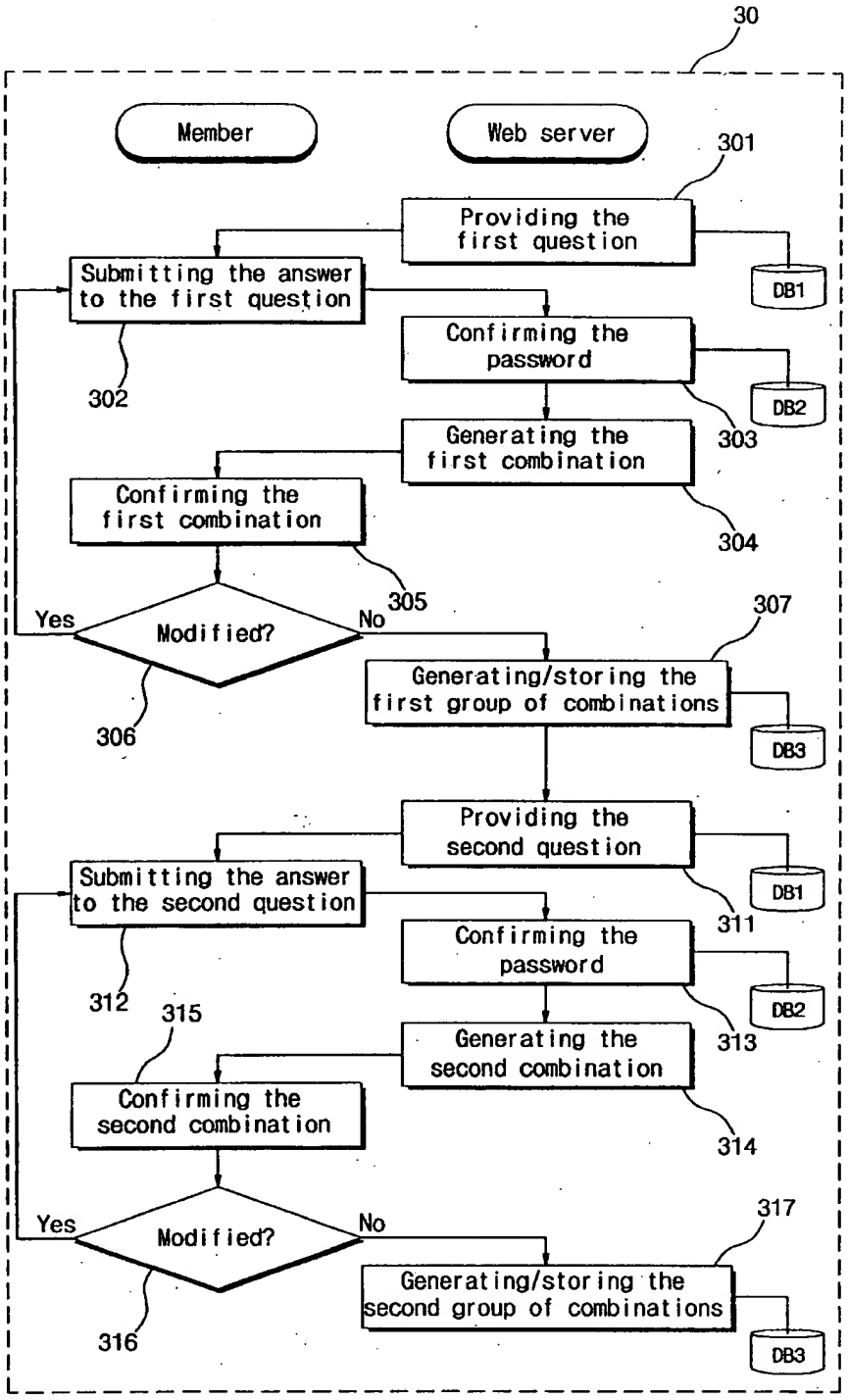

30
Member
Web server
301
Providing the first question
DB1
Submitting the answer to the first question
Confirming the password
DB2
302
303
Generating the first combination
Confirming the first combination
304
305
Yes
Modified?
No
307
306
Generating/storing the first group of combinations
DB3
Providing the second question
DB1
Submitting the answer to the second question
311
Confirming the password
DB2
312
315
313
Generating the second combination
Confirming the second combination
314
Yes
Modified?
No
317
316
Generating/storing the second group of combinations
DB3

Fig. 6

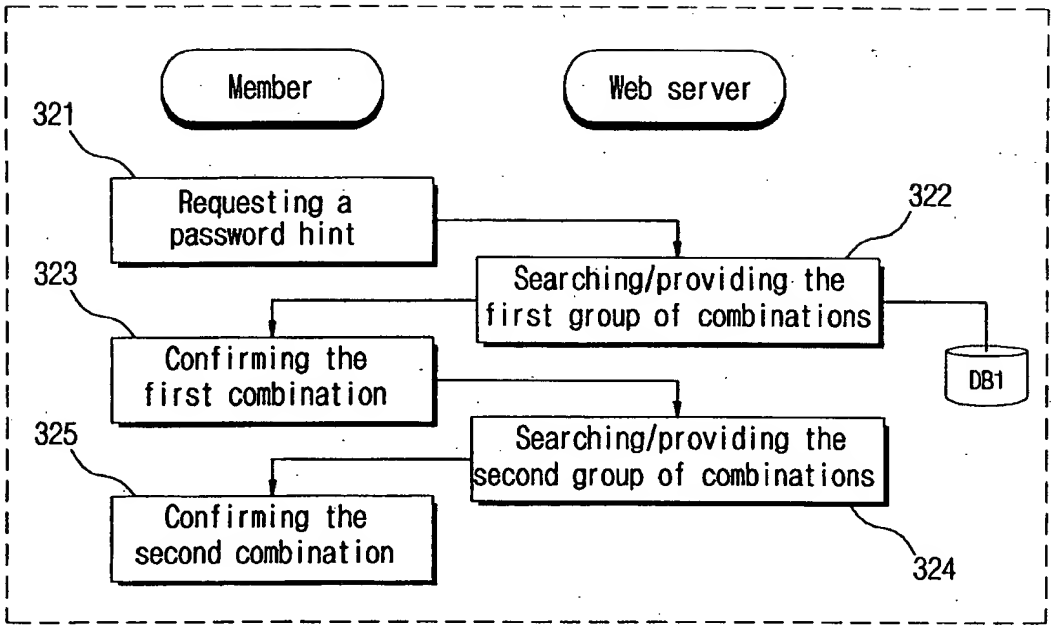

Member
Web server
321
Requesting a password hint
322
Searching/providing the first group of combinations
323
Confirming the first combination
DB1
325
Searching/providing the second group of combinations
Confirming the second combination
324

Fig. 7

This woman resembles
a star entertainer

Fig. 8

Looking carefully it is a car!

Fig. 9

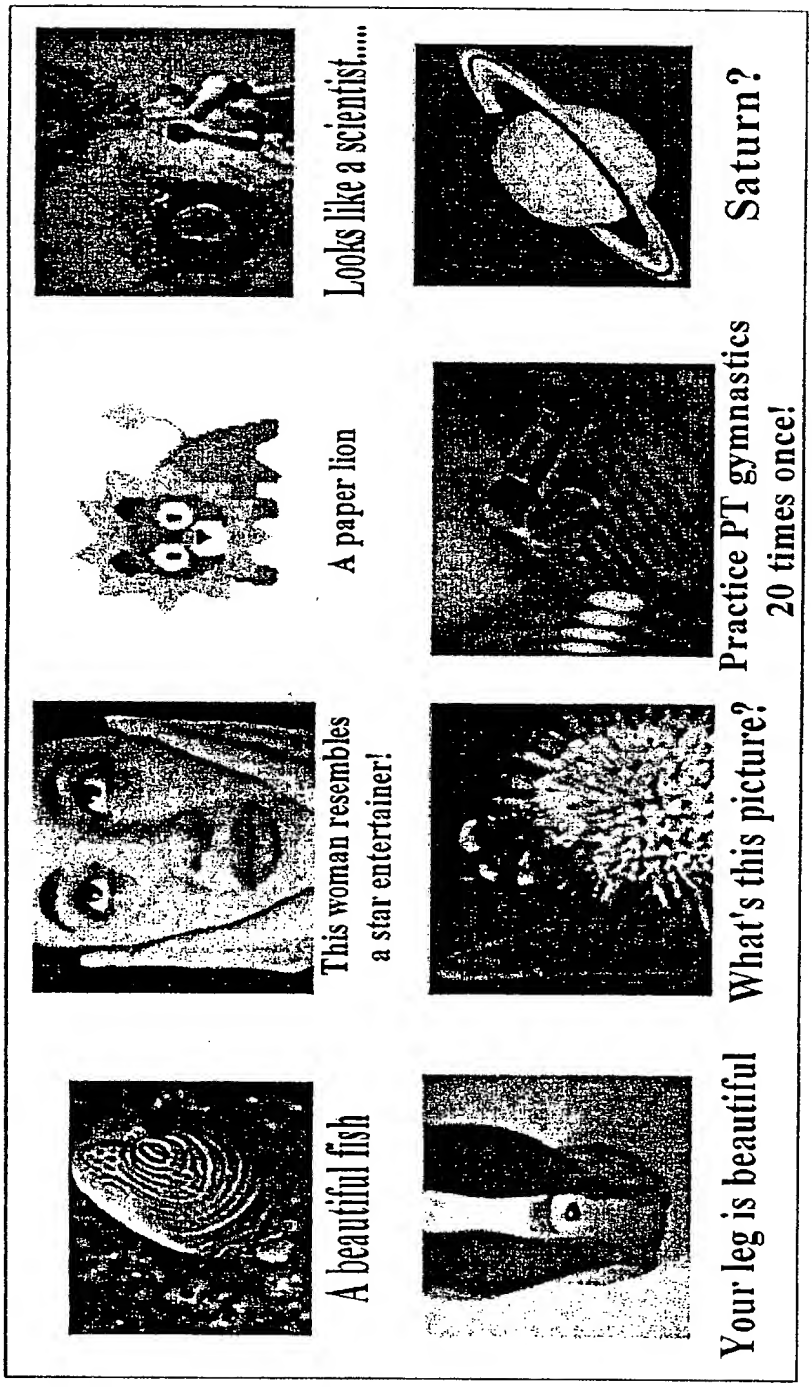
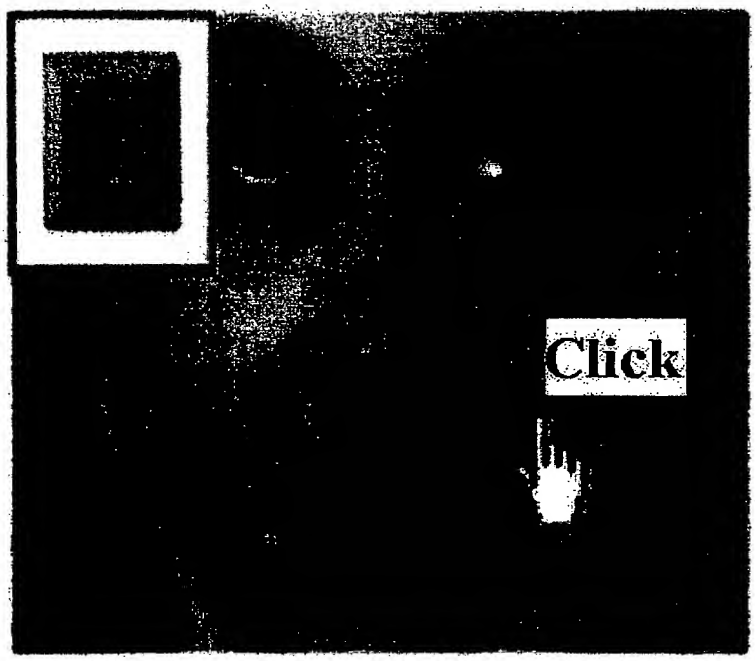
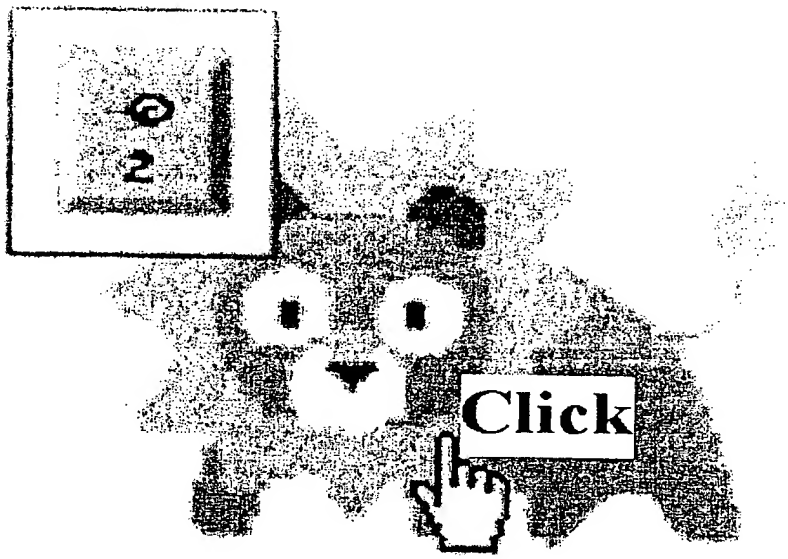

Looks like a scientist....
Saturn?
A paper lion
Practice PT gymnastics
20 times once!
This woman resembles
a star entertainer!
What's this picture?
A beautiful fish
Your leg is beautiful

Fig. 10



This woman resembles
a star entertainer

Fig. 11



A paper lion

Fig. 12

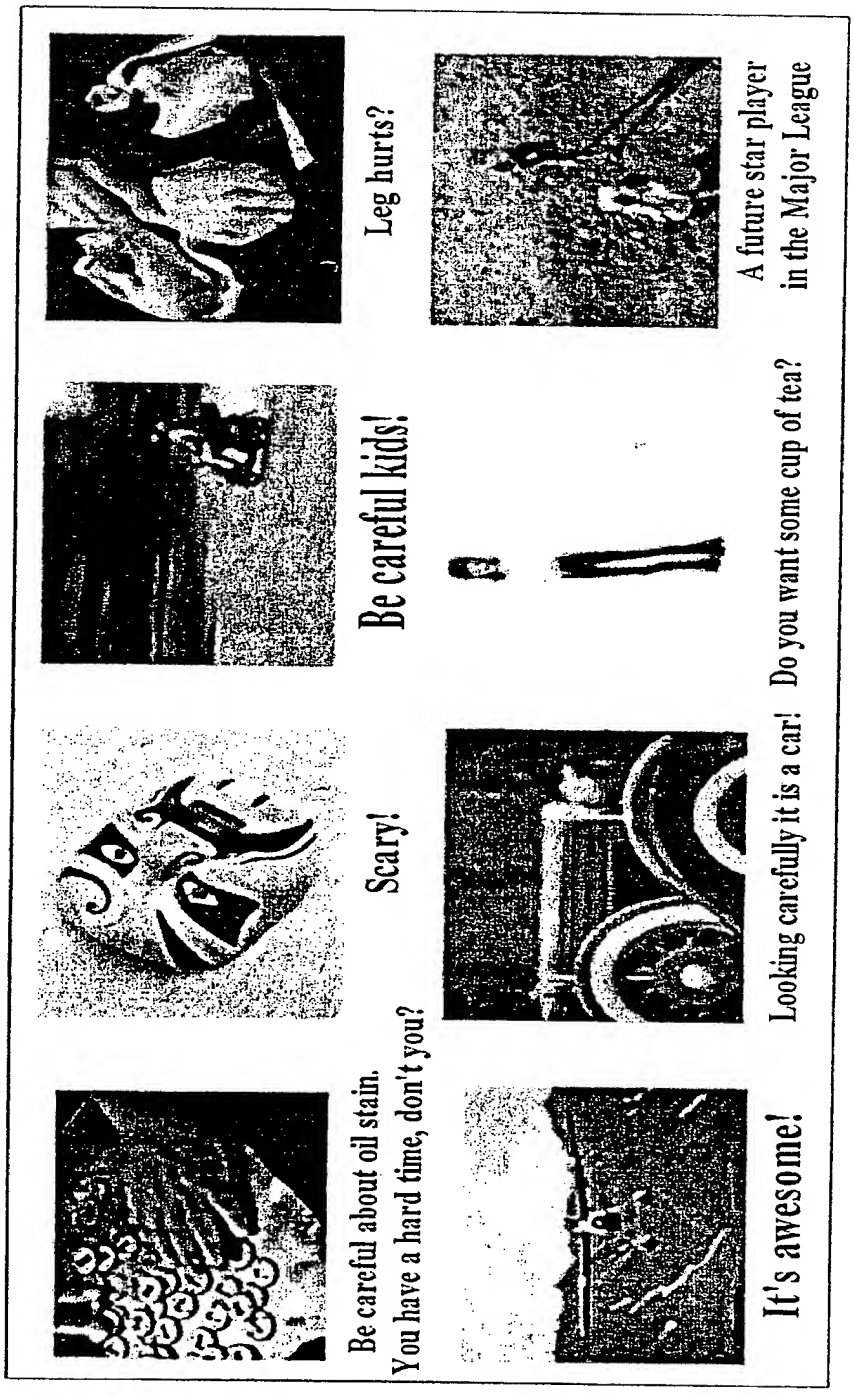
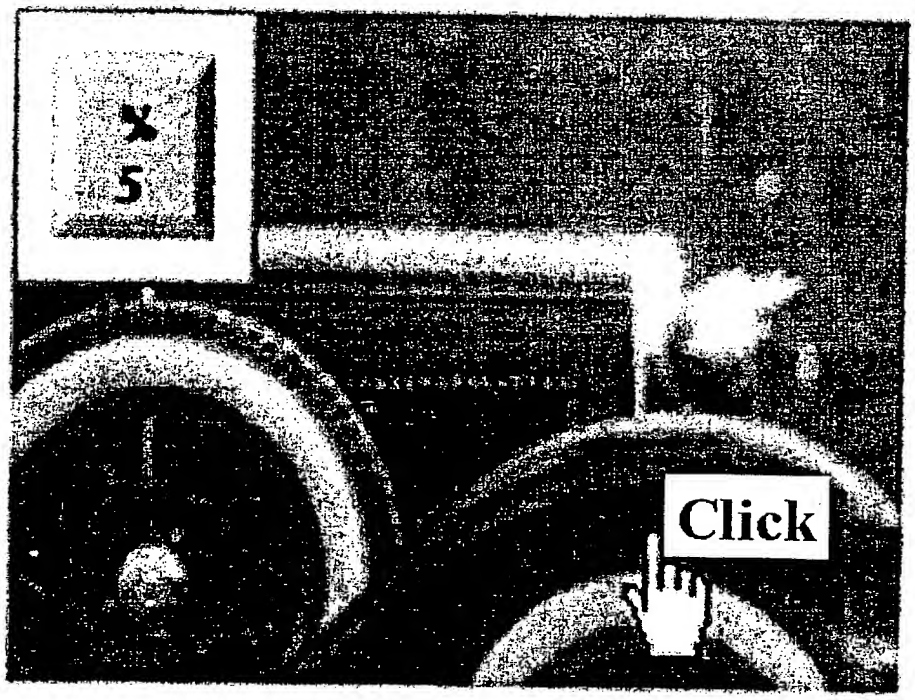
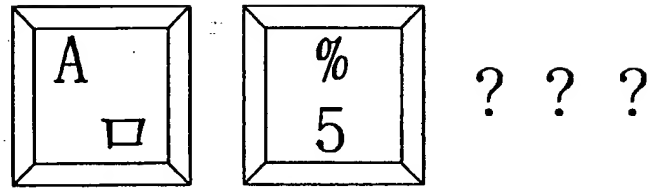

Be careful about oil stain.
You have a hard time, don't you?
Scary!
Be careful kids!
Leg hurts?
It's awesome!
Looking carefully it is a car!
Do you want some cup of tea?
A future star player
in the Major League

Fig. 13



Looking carefully it is a car!

Fig. 14



⇒ A54321

Fig. 15

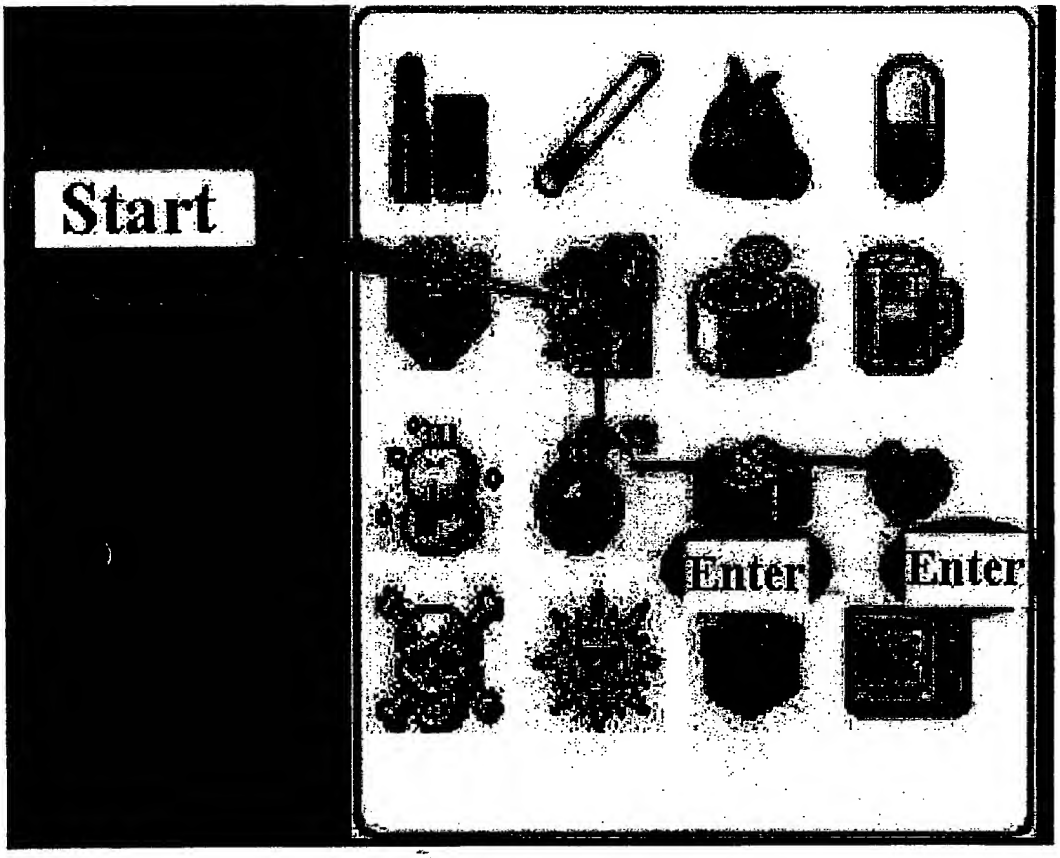
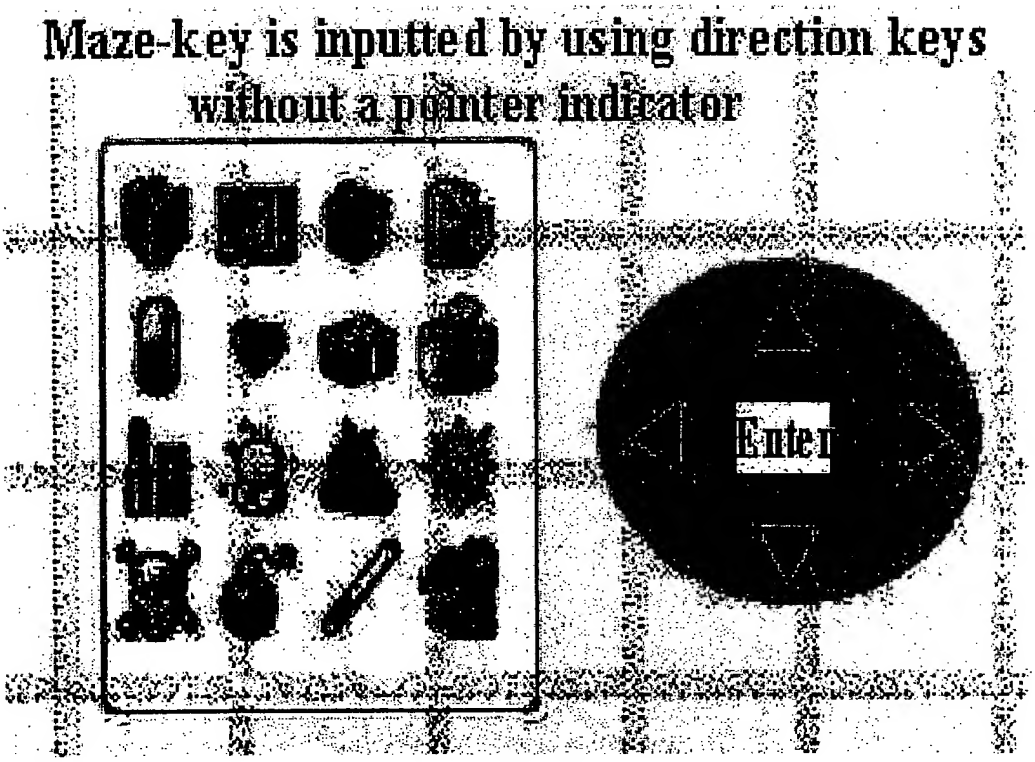


Fig. 16


Maze-key is inputted by using direction keys
without a pointer indicator
Enter

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2006/001852

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC8 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Patents and applications for inventions since 1975
Korean Utility models and applications for Utility models since 1975
Japanese Utility models and application for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

e-KIPASS, IEEE Xplore: "authentication", "question", "answer", "combination"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 2000-24087 A (KIM HAN SUNG) 6 MAY 2000 See the whole document	1,10
A	JP 15-132290 A (HITACHI LTD. , UFJ BANK LTD.) 9 MAY 2003 See the whole document	1-11
A	JP 15-50782 A (MURATA MACH LTD. , KASAHARA MASAO) 21 FEBRUARY 2003 See the whole document	1-11
A	JP 16-139221 A (NTT DOCOMO TOKAI INC.) 13 MAY 2004 See the whole document	1-11
A	JP 15-6167 A (SHARP CORP.) 10 JANUARY 2003 See the whole document	1-11

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 OCTOBER 2006 (19.10.2006)	**19 OCTOBER 2006 (19.10.2006)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	YEO, Won Hyeon Telephone No. 82-42-481-5696

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR2006/001852

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR2000-24087A	06.05.2000	None	None
JP15-132290A	09.05.2003	JP3639811B2	20.04.2005
JP15-50782A	21.02.2003	None	None
JP16-139221A	13.05.2004	None	None
JP15-6167A	10.01.2003	None	None